# Cisco FireSIGHT 시스템의 맞춤형 로컬 Snort 규칙

## 목차


[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[사용자 지정 로컬 규칙 작업](#)
[로컬 규칙 가져오기](#)
[로컬 규칙 보기](#)
[로컬 규칙 사용](#)
[삭제된 로컬 규칙 보기](#)
[로컬 규칙의 번호 지정](#)


## 소개

FireSIGHT 시스템의 사용자 지정 로컬 규칙은 로컬 시스템에서 ASCII 텍스트 파일 형식으로 가져오는 사용자 지정 표준 Snort 규칙입니다. FireSIGHT 시스템을 사용하면 웹 인터페이스를 사용하여 로컬 규칙을 가져올 수 있습니다. 로컬 규칙을 가져오는 단계는 매우 간단합니다. 그러나 최적의 로컬 규칙을 작성하려면 사용자는 Snort 및 네트워킹 프로토콜에 대한 자세한 지식이 필요합니다.

이 문서의 목적은 맞춤형 로컬 규칙을 작성하는 데 도움이 되는 몇 가지 팁과 지원을 제공하는 것입니다. 로컬 규칙 생성에 대한 지침은 snort.org에서 *제공하는 Snort Users* Manual을 참조하십시오. 사용자 지정 로컬 규칙을 작성하기 전에 Users Manual(사용자 설명서)을 다운로드하여 읽는 것이 좋습니다.

> **참고:** Sourcefire SRU(Rule Update) 패키지에 포함된 규칙은 Cisco Talos Security Intelligence and Research Group에서 생성 및 테스트하며 Cisco TAC(Technical Assistance Center)에서 지원합니다. Cisco TAC에서는 맞춤형 로컬 규칙을 작성하거나 조정하는 데 도움을 제공하지 않지만, FireSIGHT 시스템의 규칙 가져오기 기능에 문제가 있는 경우 Cisco TAC에 문의하십시오.

> **경고:** 잘못 작성된 사용자 지정 로컬 규칙은 FireSIGHT 시스템의 성능에 영향을 미칠 수 있으며, 이로 인해 전체 네트워크의 성능이 저하될 수 있습니다. 네트워크에서 성능 문제가 발생하고 FireSIGHT 시스템에서 사용자 지정 로컬 Snort 규칙이 활성화된 경우, 이러한 로컬 규칙을 비활성화하는 것이 좋습니다.

## 사전 요구 사항

### 요구 사항

Snort 규칙 및 FireSIGHT 시스템에 대한 지식이 있는 것이 좋습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- FireSIGHT Management Center(Defense Center라고도 함)
- 소프트웨어 버전 5.2 이상

## 사용자 지정 로컬 규칙 작업

### 로컬 규칙 가져오기

시작하기 전에 파일의 규칙에 이스케이프 문자가 없는지 확인해야 합니다. 규칙 가져오기를 사용하려면 ASCII 또는 UTF-8 인코딩을 사용하여 모든 사용자 지정 규칙을 가져와야 합니다.

다음 절차에서는 로컬 시스템에서 로컬 표준 텍스트 규칙을 가져오는 방법에 대해 설명합니다.

1. Policies(정책) **> Intrusion(침입) > Rule** Editor(규칙 편집기)로 이동하여 **Rule Editor(규칙 편집기) 페이지에 액세스합니다**.

2. 규칙 **가져오기를 클릭합니다**. Rule **Updates 페이지**가 나타납니다.

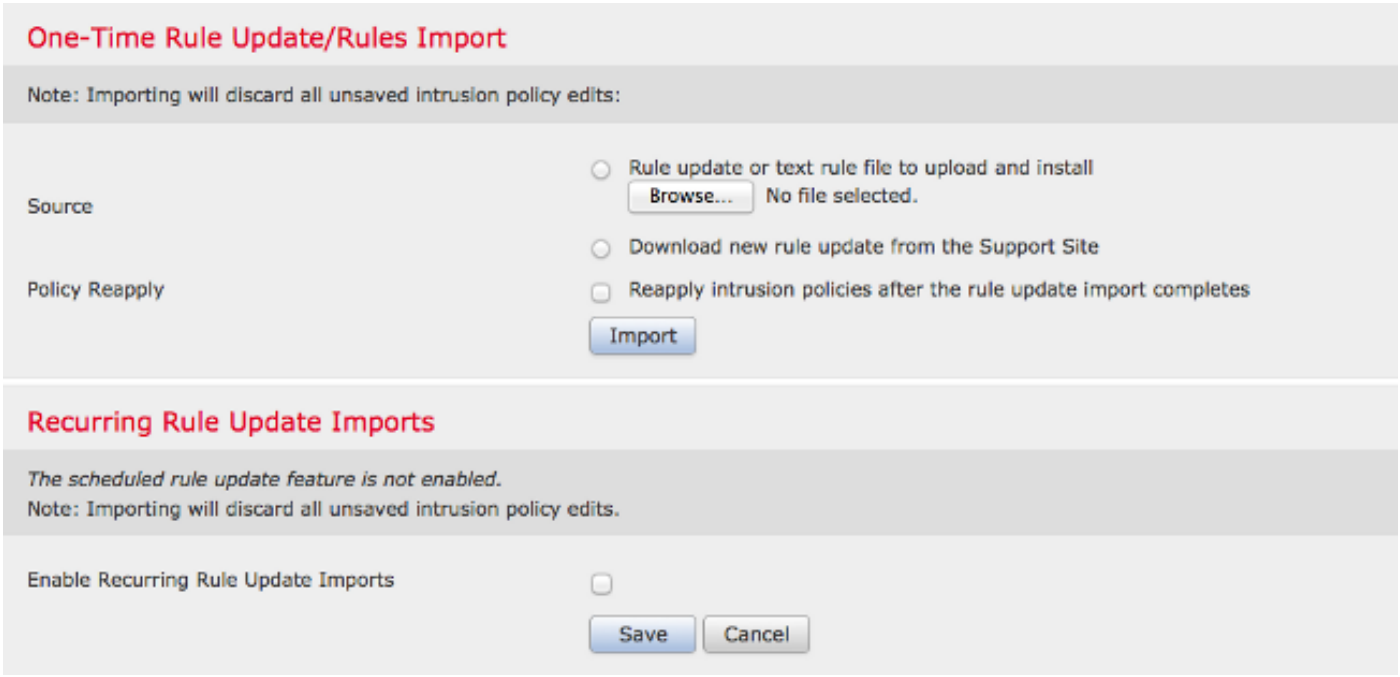



*그림: Rule Updates 페이지의 스크린샷*

3. **업로드하고 설치할 규칙 업데이트 또는 텍스트 규칙 파일을 선택하고 찾아보기**를 눌러 규칙 파일

을 선택합니다.

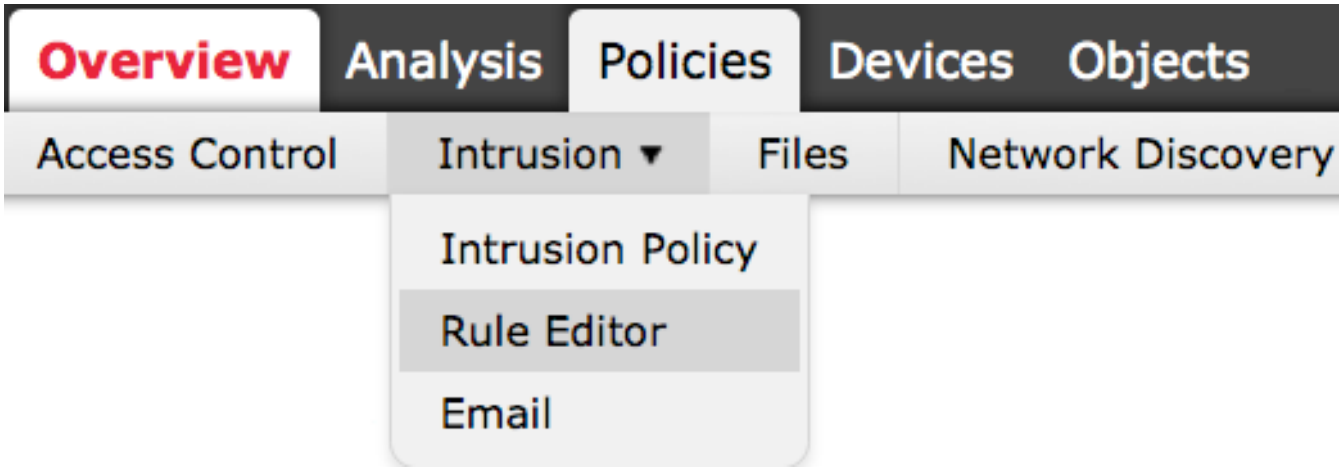
**참고:** 업로드된 모든 규칙은 **로컬 규칙 카테고리**에 저장됩니다.

4. 임포트를 **클릭합니다**. 규칙 파일을 가져옵니다.

**주의:** FireSIGHT 시스템은 검사에 새 규칙 집합을 사용하지 않습니다. 로컬 규칙을 활성화하려면 침입 정책에서 활성화한 다음 정책을 적용해야 합니다.

## 로컬 규칙 보기

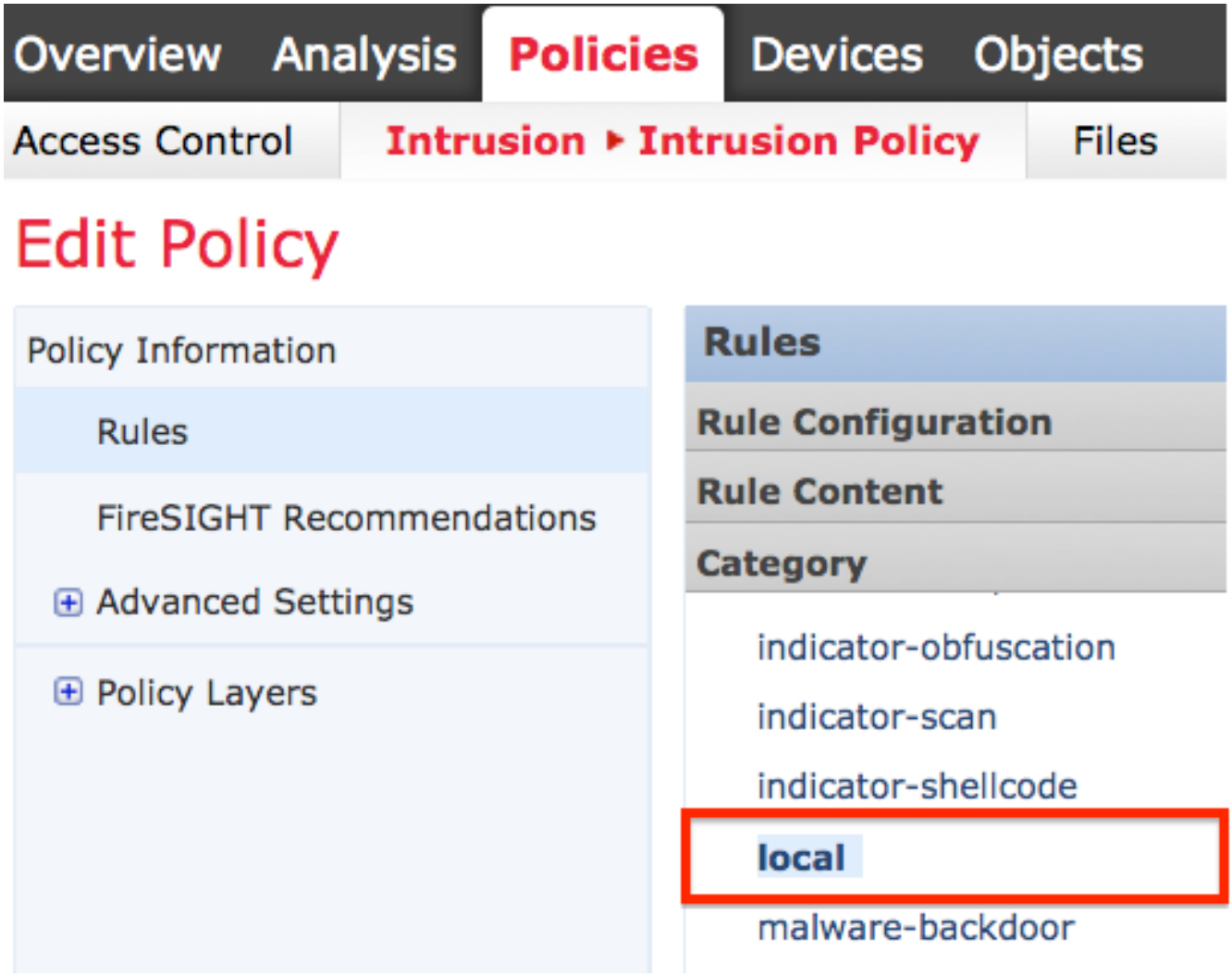
- 현재 로컬 규칙에 대한 개정 번호를 보려면 **Rule Editor** 페이지(**Policies** > Intrusion > **Rule Editor**)로 이동합니다.



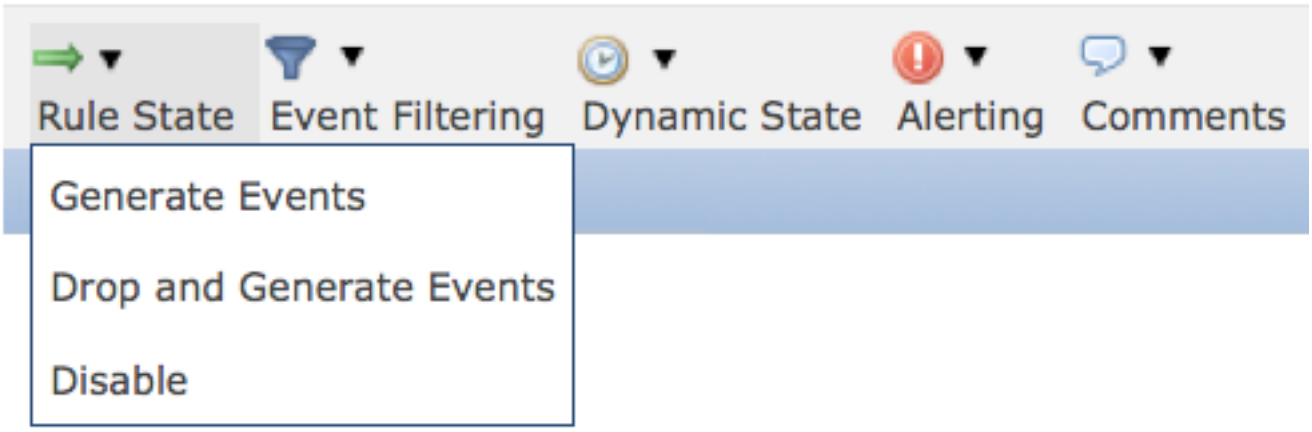

- Rule Editor(규칙 편집기) 페이지에서 **Local Rule**(**로컬 규칙**) 카테고리를 클릭하여 폴더를 확장한 다음 규칙 **옆**의 Edit(수정)를 클릭합니다.
- 가져온 모든 로컬 규칙은 자동으로 **로컬 규칙 카테고리**에 저장됩니다.

## 로컬 규칙 사용

- 기본적으로 FireSIGHT 시스템은 로컬 규칙을 비활성화 상태로 설정합니다. 침입 정책에서 로컬 규칙을 사용하려면 먼저 수동으로 로컬 규칙의 상태를 설정해야 합니다.
- 로컬 규칙을 활성화하려면 Policy Editor 페이지(Policies > Intrusion > **Intrusion** Policy)로 이동합니다. 왼쪽 **패널**에서 Rules를 선택합니다. **Category**(**카테고리**) 아래에서 local(**로컬**)을 **선택합니다**. 사용 가능한 경우 모든 로컬 규칙이 표시됩니다.




- 원하는 로컬 규칙을 선택한 후 규칙의 상태를 선택합니다.




- 규칙 상태가 선택되면 왼쪽 패널의 **Policy Information** 옵션을 클릭합니다. Commit Changes(**변경 사항 커밋) 버튼**을 선택합니다. 침입 정책이 검증되었습니다.

  **참고:** 사용되지 않는 threshold 키워드를 침입 정책의 침입 이벤트 임계값 지정 기능과 함께 사용하는 가져온 로컬 규칙을 활성화하면 정책 검증이 실패합니다.

## 삭제된 로컬 규칙 보기

- 삭제된 모든 로컬 규칙은 로컬 규칙 카테고리에서 삭제된 규칙 카테고리로 이동합니다.

- 삭제된 로컬 규칙의 개정 번호를 보려면 **Rule Editor** 페이지로 이동하여 **삭제된** 카테고리를 클릭하여 폴더를 확장한 다음 *연필 아이콘*을 클릭하여 **Rule Editor 페이지**에서 규칙의 세부 정보를 확인합니다.

## 로컬 규칙의 번호 지정

- GID(Generator)를 지정할 필요가 없습니다. 이 경우 표준 텍스트 규칙에는 GID 1만, 민감한 데이터 규칙에는 138만 지정할 수 있습니다.
- 규칙을 처음 가져올 때는 SID(Snort ID) 또는 수정 번호를 지정하지 마십시오. 이렇게 하면 삭제된 규칙을 비롯한 다른 규칙의 SID와의 충돌이 방지됩니다.
- FireSIGHT Management Center는 사용 가능한 다음 사용자 지정 규칙 SID인 1000000 이상과 수정 번호 1을 자동으로 할당합니다.
- SID가 2147483647보다 큰 침입 규칙을 가져오려고 하면 검증 오류가 발생합니다.
- 이전에 가져온 로컬 규칙의 업데이트된 버전을 가져올 때는 IPS에서 할당한 SID와 현재 개정 번호보다 큰 개정 번호를 포함해야 합니다.
- IPS에서 할당한 SID와 현재 개정 번호보다 큰 개정 번호를 사용하여 규칙을 가져와서 삭제한 로컬 규칙을 복원할 수 있습니다. 로컬 규칙을 삭제하면 FireSIGHT Management Center에서 자동으로 개정 번호를 증가시킵니다. 로컬 규칙을 복원할 수 있는 디바이스입니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.